

# DeltaCrypt Technologies inc.



## **Custom-Built Solution**

Don't let your company's special requirements keep you from protecting sensitive corporate data. Have any of the DeltaCrypt public key encryption solutions adapted to your environment.

## **Complete Range of Encryption Products**

DeltaCrypt offers a complete range of encryption applications. Whether you want to protect your PC, data exchanges, emails, USB flash memory drives as well as your backups, DeltaCrypt has the right solution for you.

## **Strong Presence in Security-conscious Organizations and Industries**

Governments, R&D, High Tech, Financial Institutions, Lotteries, Oil & Gas, etc.

## DeltaCrypt Encryption Protection

DeltaCrypt is a privately owned corporation. Our dedicated team has been developing cryptographic applications for nearly 10 years. DeltaCrypt's mission is to develop new and innovative public key encryption technologies of the highest quality suited for medium, large & enterprise clients.

### **Public Key Encryption**

DeltaCrypt applications offer public key encryption to secure exchanges and to protect sensitive files. Public key cryptography is an encryption method that uses two unique keys which are related: a public key which is used for encryption and a secret key (password) used to decrypt the data. As per its name, the public key is available to anyone wanting to cipher a message. However, the encrypted message can only be decrypted using the private key, which remains confidential.

### **1024bits RSA Keys**

At encryption, a RSA public key is used by DeltaCrypt to cipher the symmetrical key included in the encryption key. At decryption, a RSA private key is used to decipher the symmetrical key. To maintain a high level of security, DeltaCrypt does not save the RSA private key on the hard drive conversely, it generates one each time the private key is required. In both cases, DeltaCrypt uses 1024bits RSA keys.

### **Hashing**

DeltaCrypt uses a hash function to ensure the encryption integrity. All DeltaCrypt public key encryption applications benefit from a choice of hashing algorithms (SHA-1 SHA-256 and MD-5). This hashing produces a message digest to protect the encryption and the public key file integrity. For the DUSK USB protection, Encrypted Backup Solution and DEOS, DeltaCrypt strictly uses SHA-256.

### **AES Rijndael Encryption**

DeltaCrypt applications integrate the Rijndael Algorithm (128-bit, 192-bit and 256-bit keys). The high security Rijndael algorithm is the new Advanced Encryption Standard (AES) chosen by the National Institute of Standards and Technology (NIST, FIPS-197).

### **FIPS 140-2 Certification**

DeltaCrypt is currently undergoing a FIPS 140-2 Certification. The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules.

### **Patent-pending technology**

DeltaCrypt DUSKWatch is patent-pending.

# DUSKWatch to Control USB mobile devices

If your organization is concerned about its mobile data on USB Mobile Devices or any other USB mass storage peripherals, the DeltaCrypt DUSKWatch application will let you control the USB drives on which your corporate data is copied to.

Used alone, DUSKWatch will not permit the copying of corporate data out to unprotected USB mass storage peripherals. Used in conjunction with DUSK protected drives or hard disks, DUSKWatch can only allow Users to access and copy files on such protected USB devices. DeltaCrypt DUSKWatch is patent-pending.

## DUSKWATCH FEATURES

### **Get the Assurance that Corporate Mobile Data is Protected at All Time**

As soon as the computer is turned on, DUSKWatch blocks all unprotected USB Mass storage devices. If configured, it authorizes the copy of data only when a personalized DUSK-protected USB device is detected. Not only does the USB mass storage device need to be DUSK-protected, but the protection must be personalized to your organization. Without this double recognition, no copy on any USB drives will be granted.

### **Blocks Unauthorized Mobile Devices**

DUSKWatch may be configured to block unauthorized and unprotected USB devices such as USB flash drives, USB hard disks, memory card, iPods and cameras to name a few.

### **Other Mobile Devices Controlled **Coming soon****

An IT Administrator will shortly be able to configure DUSKWatch to block unauthorized Bluetooth devices, Wi Fi devices and Infra Red devices.

### **Read Files from Unprotected Mass Storage Devices**

When set, clicking on the DUSKWatch icon in the computer tray and selecting the read-only mode, Users will be able to see, consult and copy files from the next unprotected device to be connected to the computer without needing to disable DUSKWatch control. Even when the read-only mode is activated, DUSKWatch will keep Users from copying data out on such unprotected devices.

### **Transparent to your Users**

Once installed on your Users' workstations, DUSKWatch becomes completely transparent to them. DUSKWatch works quietly in the background. No training is needed!

### **DUSK Protection Utility Tool **New****

When used with DUSK protection for USB drives, DUSKWatch can update DUSK protection so that you don't have to recuperate all drives in circulation within your organization and without any User intervention.

When DUSK decentralized installation is preferred, DUSKWatch can enable Users to install DUSK protection onto their USB drives by placing a DUSK installer icon on their desktop. Double clicking on the icon will automatically launch DUSK installation.

### **Active Directory Configuration **New****

With the .ADM file inserted to the Active Directory Group Policy Management, DUSKWatch options are easily configured by the IT Administrator. From DUSK protection icon on Users' desktop to the read-only mode of unprotected devices, DUSKWatch configuration is shaped according to your security needs.

### **DUSKWatch Log Journal **New****

DUSKWatch may be configured to gather logs of protected and unprotected devices that are connected to your network.

### **Illegal Intrusion Attacks**

DUSKWatch can inform management if an unprotected USB drive or hard disk was connected to a workstation to help an organization determine which workstation is more vulnerable to illegal intrusion attacks.

DUSKWATCH SPECS	
Operating systems	Windows 2000, Win Server 2003, XP and Vista <b>New</b>
Application volume size:	3.1 MB
Security	<ul style="list-style-type: none"> <li>• Authorizes DUSK-protected USB mass storage devices</li> <li>• Blocks any unprotected and unauthorized USB mass storage devices</li> <li>• Read-only option for unprotected USB mass storage devices</li> </ul>
Use	Transparent to User. Automatically launched when opening a session, unlimited privileges (Administrator account) and limited privileges (User account)
Distribution	Download
Installation	MSI file, unlimited privileges required (Administrator account)
Active Directory Configuration (Activation / deactivation)  Policies applicable to : <ul style="list-style-type: none"> <li>- User groups</li> <li>- Workstation groups</li> </ul>	<ul style="list-style-type: none"> <li>• Blocks USB mass storage devices               <ul style="list-style-type: none"> <li>○ USB Flash drives</li> <li>○ USB HDD</li> <li>○ Firewire</li> <li>○ Memory card readers</li> <li>○ Cameras</li> <li>○ iPods ...</li> <li>○ Bluetooth devices <b>Coming soon</b></li> <li>○ WiFi devices <b>Coming soon</b></li> <li>○ Infra Red devices <b>Coming soon</b></li> </ul> </li> <li>• Blocks floppy disks</li> <li>• Blocks CD-ROMs/DVDs</li> <li>• Installation icon on desktop</li> <li>• Log recording</li> <li>• Log parameters</li> <li>• Read-only mode of unprotected devices</li> <li>• Authorised devices black list</li> <li>• Device white list</li> <li>• Language</li> <li>• DUSK Protection Utility tool               <ul style="list-style-type: none"> <li>○ DUSK installation icon on desktop</li> <li>○ DUSK updates (if needed)</li> <li>○ Master Key modification</li> </ul> </li> </ul>
Updates	12 months included.

**Control USB drives within your corporate environment with DUSKWatch solution now!**

## INSTALLATION

You may choose to have Users install DUSKWatch on their workstation or you may decide to have your IT Administrator remotely install DUSKWatch on all workstations.

### USER INSTALLATION

#### From Unlimited Privilege Computers

If you prefer to have Users perform DUSKWatch installation, all they will have to do is execute the .msi file on their workstation.

### ADMINISTRATOR INSTALLATION

#### Using GPO or SMS

If DUSKWatch installation is remotely performed by your IT Administrator, DUSKWatch .msi installer can be pushed using GPO or SMS.

## Custom-Built Solution

Don't let your specific requirements keep you from protecting your sensitive data, contact DeltaCrypt instead. It will be our pleasure to study the possibility to adapt our technology to meet your special needs.



### Contact us

DeltaCrypt Technologies Inc.

By phone at 1-888-500-3563

By email at [dtiinfo@deltacrypt.com](mailto:dtiinfo@deltacrypt.com)